1. A method for enhancing the security of information, comprising the steps of:

gathering at least two plaintext messages, each plaintext message containing information; and

creating an encrypted mux message from the at least two plaintext messages, such that the encrypted mux message comprises encryptions of the at least two plaintext messages and the encrypted mux message has characteristics which disguise the encrypted mux message as an encryption of fewer plaintext messages than it actually contains.

2. The method of claim 1, wherein the creating step creates an encrypted mux message which has at least four of the following characteristics in common with an encryption of a single plaintext message: syntax, file name, file name extension, creation date, modification date, length, header, checksum, digital signature, storage directory.

3. The method of claim 1, wherein the creating step creates an encrypted mux message which has at least three of the following characteristics in common with an encryption of a single plaintext message: syntax, file name, file name extension, length, header, checksum, digital signature, storage directory.

4. The method of claim 1, further comprising the step of choosing a plaintext message to be revealed, the chosen plaintext message having an encryption in the encrypted mux message.

5. The method of claim 4, further comprising the step of making available to an unauthorized party a key for the chosen plaintext message, thereby permitting the unauthorized party to obtain the information in the chosen plaintext message by decrypting a portion of the encrypted mux message without permitting the unauthorized party to decrypt another portion of the encrypted mux message.

6. A method for use in a software program to enhance the security of information, comprising the steps of:

accepting a key from a user;

using the key to find a corresponding message encryption in a file containing encryptions of at least two plaintext messages, the file being disguised to resemble a file containing fewer encryptions than are actually present in the file;

decrypting the corresponding message encryption; and

making plaintext available to the user.

7. The method of claim 6, wherein the step of using the key to find a corresponding message encryption uses a field in the key to find the corresponding message encryption.

8. The method of step 7, wherein the field specifies a label located in the file to identify the corresponding message encryption.

9. The method of step 7, wherein the field specifies a string in the plaintext of the corresponding message encryption.

10. The method of step 6, wherein the step of making plaintext available to the user comprises at least one of the following: displaying the plaintext on a computer screen, saving a copy of the plaintext in a file, transmitting a copy of the plaintext over a network.

11. The method of step 6, wherein the step of making plaintext available to the user makes available the plaintext for the message encryption corresponding to the key provided.

12. The method of step 6, wherein the step of making plaintext available to the user makes available a watermarked version of the plaintext for the message encryption corresponding to the key provided.

13. The method of step 6, further comprising the step of sending a silent alert.

14. An article comprising a computer-readable medium configured with an embodied encrypted mux message that is disguised to hide at least one encryption and that is also susceptible of being at least partially decrypted in response to provision of a key corresponding to an encryption of plaintext within the encrypted mux message.

15. The article of claim 14, wherein the encrypted mux message is structured to contain contiguously stored message encryptions.

16. The article of claim 14, wherein the encrypted mux message is structured to contain interleaved stored message encryptions.

17. The article of claim 14, wherein the encrypted mux message contains message selection hints.

18. A computer system comprising a storage medium configured by an encrypted mux message stored therein, and a software security enhancing means for enhancing the security of information by using the encrypted mux message.

19. The system of claim 18, wherein the security enhancing means comprises software for creating an encrypted mux message from at least two plaintext messages.

20. The system of claim 18, wherein the security enhancing means comprises software for accepting a key from a user; using the key to find a corresponding message encryption in the encrypted mux message; decrypting the corresponding message encryption; and making plaintext available to the user.